UDC 004.9

PROTOCOLS IN IOT: ASSESSMENT AND ENHANCEMENT

Toktosunova Z.
specialist degree, I. Razzakov Kyrgyz State Technical University (Bishkek, Kyrgyzstan)

ПРОТОКОЛЫ БЕЗОПАСНОСТИ В IOT: ОЦЕНКА И УЛУЧШЕНИЕ

Токтосунова З.А.
специалист, Кыргызский государственный технический университет им. И. Раззакова (Бишкек, Кыргызстан)

Abstract

This paper examines the main security protocols used in the Internet of Things (IoT) and analyzes methods aimed at improving data and device protection. With the growth of IoT devices, the risk of cyberattacks increases, necessitating specialized protocols like TLS, DTLS, and MQTT. TLS and DTLS provide reliable data encryption at the transport layer, though their high resource requirements limit usage in low-power devices. MQTT, optimized for low-resource devices, supports built-in authentication and encryption functions, making it popular for IoT networks. The paper also considers lightweight cryptography to enhance security with limited computational capacity and distributed access management systems based on blockchain. The combination of security protocols and adaptive methods achieves high resilience in IoT networks, enhancing overall system security and reliability.

Keywords: IoT security, TLS protocol, MQTT, DTLS, lightweight cryptography, access management.

Аннотация

В статье рассмотрены основные протоколы безопасности, используемые в интернете вещей (IoT), и проанализированы методы, направленные на улучшение защиты данных и устройств. С увеличением числа IoT-устройств возрастает риск кибератак, что требует применения специализированных протоколов, таких как TLS, DTLS и MQTT. TLS и DTLS обеспечивают надежное шифрование данных на транспортном уровне, хотя их ресурсоемкость ограничивает возможности использования в условиях ограниченных ресурсов. MQTT, оптимизированный для маломощных устройств, поддерживает встроенные функции аутентификации и шифрования, что делает его популярным для IoT-сетей. В статье также рассматривается легковесная криптография для повышения безопасности в условиях низких вычислительных мощностей, а также распределённые системы управления доступом, основанные на блокчейне. Применение комбинации протоколов безопасности и адаптивных методов позволяет достичь высокой устойчивости IoT-сетей, что повышает общую защищенность и надежность системы в целом.

Ключевые слова: безопасность IoT, протокол TLS, MQTT, DTLS, легковесная криптография, управление доступом.

Introduction

With the rise of the Internet of Things (IoT) and its integration across various sectors, including industry, healthcare, and consumer electronics, the need for securing IoT networks and devices is growing. IoT systems, which connect numerous sensors and devices into a single network, pose significant security risks, as each connected object can become a potential point of attack. Due to the

limited computational power and memory of most IoT devices, traditional security methods often prove ineffective or too resource-intensive. This article aims to examine existing security protocols for IoT and analyze methods that can enhance protection in this rapidly evolving field. One of the primary challenges for IoT protocol developers is ensuring data privacy and integrity with minimal computational resource usage. In networks composed of numerous resource-constrained devices, developing reliable protocols becomes particularly critical. In practice, this means that IoT security protocols must protect against external threats and be resilient to internal failures. This article reviews major security protocols, such as Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), and Lightweight Cryptography, their strengths and limitations, and offers recommendations for optimizing them. With the rise in cyberattacks targeting IoT devices, there is a need to analyze potential vulnerabilities and find solutions to strengthen IoT systems' resilience. This requires using flexible, scalable, and easily adaptable protocols that can integrate into various IoT networks and meet security requirements. The article examines both existing and emerging protection methods, including hybrid authentication schemes, distributed access control systems, and adaptive encryption algorithms. These approaches enhance IoT security and ensure stable network operation even as complexity increases.

Main part

One widely used protocol for securing data in IoT networks is Transport Layer Security (TLS), which encrypts data at the transport protocol level. TLS ensures data confidentiality and integrity, making it beneficial for networks with limited access. However, due to its resource-intensive nature, TLS may not be suitable for IoT devices with limited computational capabilities. In such cases, a lighter protocol version, Datagram Transport Layer Security (DTLS), is used. DTLS is specifically designed for data transmission in resource-constrained networks and supports encryption without significant device load [1].

As data may traverse numerous nodes in IoT networks, authentication becomes essential. A common approach for IoT authentication is Lightweight Cryptography, which is developed for devices with limited resources. Lightweight cryptography includes algorithms requiring minimal memory and processing power while providing a basic level of security. Examples include SPECK and Simon, which support symmetric data encryption.

Another critical aspect of IoT security is device access control [2]. In traditional networks, access control is centralized through servers, but a more suitable solution for IoT involves Distributed Access Control, allowing IoT devices to autonomously manage access without constant connection to a central server. Blockchain-based protocols are also considered a potential solution for secure access management in IoT networks, as they provide secure, immutable access records.

The Message Queuing Telemetry Transport (MQTT) protocol, which supports data protection through built-in authentication and encryption mechanisms, is used to monitor IoT device security. MQTT enables IoT devices to send and receive messages with flexibility and minimal delays [3]. An example Python code demonstrating device connection to an MQTT broker with authentication is shown below:

```
import paho.mqtt.client as mqtt

# MQTT Settings
broker = "mqtt.example.com"
port = 8883  # SSL/TLS port
username = "user"
password = "password"

# Function for SSL/TLS connection
def on_connect(client, userdata, flags, rc):
    if rc == 0:
        print("Connection successful")
    else:
```

```
        print("Connection failed, code:", rc)

    # Initialize MQTT client
    client = mqtt.Client()
    client.username_pw_set(username, password)
    client.tls_set()  # Use TLS for security
    client.on_connect = on_connect

    # Connect to MQTT broker
    client.connect(broker, port)
    client.loop_start()
```

This code demonstrates how an IoT device can connect to an MQTT broker using SSL/TLS. Authentication via MQTT ensures secure data transmission and enables the device to exchange information with other network components.

In addition to basic security, identifying anomalies and preventing attacks are crucial. Adaptive machine learning methods, which detect abnormal behavior, are used for this. These methods analyze network traffic and sensor data, identifying suspicious activity like excessive activity or unauthorized access [4]. Thus, combining security protocols with machine learning algorithms allows for a comprehensive IoT protection system, resilient to modern threats and capable of real-time data security. Figure 1 depicts the adoption trends of IoT security protocols over recent years, showing a steady increase in their implementation to secure IoT networks.

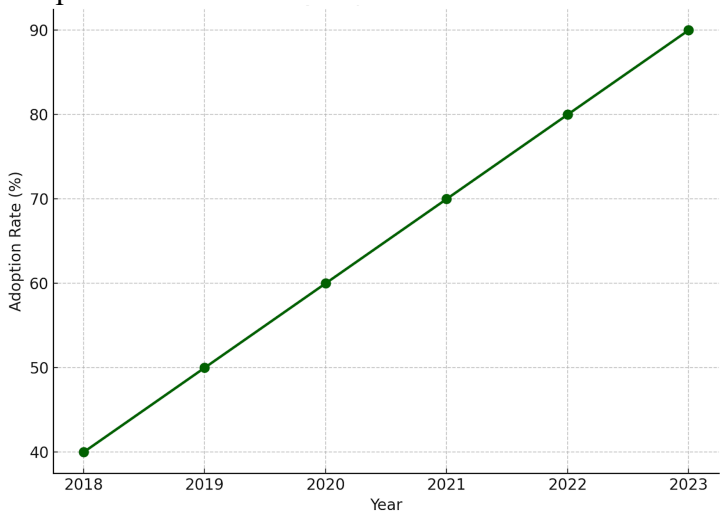

Figure 1. IoT security adoption trends over time

Figure 1 highlights a significant growth in IoT security protocol adoption, rising from 40% in 2018 to 90% in 2023. This trend reflects increasing awareness and prioritization of security measures in IoT networks. The steady increase underscores the necessity for scalable and efficient protocols to meet the growing demand for secure IoT environments.

Evaluation of IoT security protocols

Effective protection of devices and data in IoT networks requires specialized security protocols ensuring reliable data transmission and storage. IoT security protocols such as TLS (Transport Layer Security), DTLS (Datagram TLS), and MQTT (Message Queuing Telemetry Transport) play a vital role in minimizing risks related to data leaks and unauthorized access. TLS and DTLS provide secure data transmission at the network level, using encryption to protect data integrity and confidentiality. This is especially important in IoT, where devices often exchange sensitive data [5].

MQTT is a message exchange protocol widely used in IoT for transmitting data from devices to a server. Its built-in security mechanisms include client authentication and encryption support, making it ideal for situations where minimal latency and high transmission speed are required. The protocol also supports lightweight connection models, which are optimal for resource-constrained IoT devices [6].

Evaluating these protocols' effectiveness in IoT networks shows that their combined use achieves a high level of network security and resilience.

For example, TLS and DTLS provide transport-level security, particularly relevant for applications requiring reliable and secure connections. However, applying these protocols may impose significant load on devices with limited computational resources, requiring optimization [7]. Figure 2 illustrates the effectiveness of commonly used IoT security protocols, including TLS, DTLS, and MQTT, highlighting their relative performance in securing IoT networks.

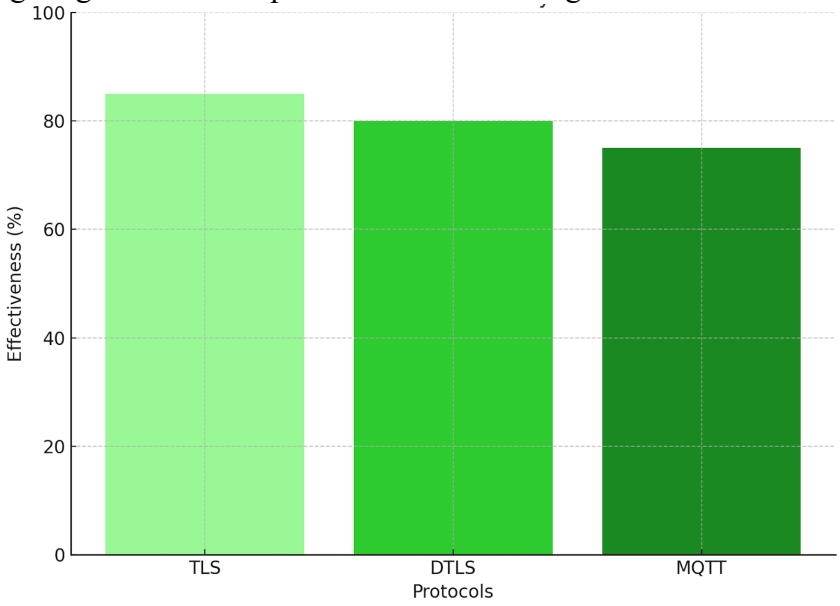

Figure 2. Effectiveness of IoT security protocols

As shown in Figure 2, TLS provides the highest level of effectiveness at 85%, ensuring robust data encryption for secure connections. DTLS follows with 80%, offering lightweight encryption suitable for resource-constrained IoT devices. MQTT, while slightly lower at 75%, demonstrates sufficient effectiveness for secure message exchanges with minimal latency. This comparison underscores the importance of selecting the appropriate protocol based on network requirements and device capabilities.

Conclusion

As the Internet of Things evolves rapidly, securing IoT networks and devices becomes a top priority. Security protocols such as TLS, DTLS, and MQTT demonstrate high potential for protecting data transmitted between devices, but their application requires consideration of IoT network specifics. TLS and DTLS, which provide transport-level security, are suitable for networks with high-security demands, though they have limitations on resource-constrained devices.

Effective implementation of IoT security protocols requires balancing protection level with device computational capacity. Using lightweight cryptographic methods and optimizing protocols like MQTT reduce device load while maintaining high security. Moreover, integrating adaptive data analysis methods and machine learning improves monitoring and allows for timely threat detection.

Thus, enhancing IoT network security requires a comprehensive approach, combining security protocols, adaptive protection methods, and distributed access control systems. These measures create robust, secure IoT networks capable of functioning effectively under high demands for data reliability and confidentiality.

References

1. Naraliev N.A., Samal D.I. Review and analysis of standards and protocols in the field of the Internet of Things. Modern testing methods and IoT information security issues // International Journal of Open Information Technologies. 2019. Vol. 7. No.8. P. 94-104.
2. Kazhenova Zh.S., Kenzhebaeva Zh.E. Security in IoT protocols and technologies: a review // International Journal of Open Information Technologies. 2022. Vol. 10. No.3. P. 10-16.

3. Umarov A., Mukhtoriddinov M., Ismoilov S. IoT security protocols: analysis, vulnerabilities, and prospects // Conference on Digital Innovation: "Modern Problems and Solutions". 2023.
4. Fomicheva V.A., Parotkin N.Yu. Review of technologies for ensuring the security of IoT device operation // Current Issues in Aviation and Cosmonautics. 2022. Vol. 2. P. 318-320.
5. Baev D.A., Volkov R.O., Zonov A.D. Security monitoring in IoT networks // StudNet. 2021. Vol. 4. No.6. P. 1119-1126.
6. Ermakov S.A., Bolgov A.A., Mokrousov A.N. Assessment of IoT network protection efficiency using the example of smart home technology // Information and Security. 2019. Vol. 22. No.1. P. 130-133.
7. Hofer-Schmitz K., Stojanović B. Towards formal verification of IoT protocols: A Review // Computer Networks. 2020. Vol. 174. P. 107233.